Section IV: **Administrative Security**
Title: **Information System Certification and Accreditation Standard**
Current Effective Date: **June 30, 2008**
Revision History: **June 17, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To ensure that all North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices implement security into Information System Certification and Accreditation processes.

STANDARD

1.0 Background

The Divisions and Offices management shall ensure that information systems are properly certified and accredited by developing Information Certification and Accreditation policies, procedures and guidelines based on a five (5) phase process.

2.0 Information System Certification and Accreditation Phases

The Divisions and Offices must adhere to the following phases when certifying and accrediting information systems:

- Initiation Phase
- Certification Phase
- Accreditation Phase
- Monitoring Phase
- Reauthorization Phase

2.1 Initiation Phase

The Divisions and Offices management must determine the required resource effort that will be necessary to complete the Information System Certification and Accreditation phases. The Divisions and Offices must identify, document, secure, and safeguard the following resource efforts:

- A cost analysis report must be completed, which will dictate the cost associated with completing the Information System Certification and Accreditation phases.
- An estimated amount of workforce members needed to complete the Information System Certification and Accreditation phases must be completed.

2.2 Certification Phase

In order to complete the Certification Phase, the Divisions and Offices must have assigned workforce members conduct the three (3) tiered Risk Management Guide. The three (3) tiered Risk Management Guide is found in the NC DHHS Security Standards, Administrative Security Standards – Information Security Risk Management Standard. The Divisions and Offices must create and/or assemble any information system security plan documentation. For assistance in creating and/or assembling the information system security plan documentation, see the NC DHHS Security Standards Manual, Application Security Standards – Information System Security Plan Standard.

Upon conducting the three (3) tiered Risk Management Guide, the Divisions and Offices management must ensure that the following criteria are identified, documented, secured, and safeguarded:

- The security category of the information system must be classified as *low*, *moderate*, or *high* impact. The security category will be found upon creating and/or assembling the Divisions and Offices information system security plan. The security categories must focus on the magnitude of harm that would occur if information system confidentiality, integrity, or availability was comprised.
  - For more information concerning security category determination, refer to the NC DHHS Security Standards, Application Security Standards – Information System Security Plan Standard. The Division and Office management must be aware that a higher security category determination will require a higher level of resource support.
- The potential threats to the information system vulnerabilities need to be identified. The potential threats will be identified in the three (3) tiered Risk Management Guide.
  - For additional information, refer to Section 5.1: Phase I – Identify Risks, in the NC DHHS Security Standards, Administrative Security Standards – Information Security Risk Management Standard.
- The information system vulnerabilities that could be exploited by potential threats need to be identified. Information system vulnerabilities will be found in the three (3) tiered Risk Management Guide.
  - For additional information, refer to Section 5.1: Phase I – Identify Risks, in the NC DHHS Security Standards, Administrative Security Standards – Information Security Risk Management Standard.
- The proper security controls must be identified and documented. Proper security controls will be identified in the three (3) tiered Risk Management Guide. The Divisions and Offices management must ensure that the risk determined after identifying and documenting security controls is acceptable.
  - For additional information, refer to Section 5.3: Phase III – Risk Management, in the NC DHHS Security Standards, Administrative Security Standards – Information Security Risk Management Standard.

2.3 Accreditation Phase

In order to accredit an information system, the DHHS Divisions and Offices management and assigned workforce members must analyze the risks associated with an information system's threats and/or vulnerabilities. The Divisions and Offices management must determine the final accreditation decision by using the below criteria:

- If appropriate security controls have been implemented, and the risk associated with the information system threats and/or vulnerabilities is *acceptable*, then the Division or Office management must grant authority to implement the information system. Once implemented, the Accreditation Phase will end and the Divisions and Offices management must ensure the remaining Certification and Accreditation Phases are completed.
- If appropriate security controls have been implemented, and the risk associated with the information system threats and/or vulnerabilities is *unacceptable*, then the Division or Office management may issue interim approval to operate. Interim approval to operate will allow the Division or Office to implement the information system into the production environment, as long as appropriate security controls will be implemented at a time agreed upon by Division or Office management.
- If appropriate security controls have been implemented, and the risk associated with information system threats and vulnerabilities is *unacceptable*, then the Division or Office management must not grant accreditation for the information system. If the information system is not accredited, the Accreditation Phase will end.

The Divisions and Offices management must ensure that the Division Information Security Officials (ISO) document, secure, and safeguard the accreditation decision against any type of tampering or malice. The Divisions and Offices management must determine the appropriate workforce members that must receive copies and/or notification of the accreditation decision per occurrence.

2.4 Monitoring Phase

Assigned DHHS workforce members must monitor actual and/or potential information system changes periodically. The monitoring of information system changes must occur throughout an information system's lifecycle. The Divisions and Offices must follow the NC DHHS Security Standards, Administrative Security Standards – Information Security Change Management Standard.

The changes to information systems may affect the implementation of the information system security controls. DHHS workforce members must monitor information system security controls routinely in order to ensure that all security controls are producing the desired outcome, being implemented correctly, and operating as intended. Updates to the information system security controls must be documented in the information system security plan and in the three (3) tiered Risk Management Guide.

2.5 Reauthorization Phase

The Divisions and Offices management are responsible for conducting information system reauthorization. Information systems must be reauthorized at least once every three (3) years or when changes to information systems adversely affect the Divisions and Offices security environment. The Reauthorization Phase entails a new Information System Certification and Accreditation process, beginning with the Initiation Phase.

References

- Department of Health and Human Services, Centers for Medicare and Medicaid Services, Version 1.0, May 12, 2005

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Security Change Management Standard
    - Information Security Risk Management Standard
  - Application Security Standards
    - Information System Security Plan Standard